PUNE RESEARCH SCHOLAR ISSN 2455-314X
AN INTERNATIONAL MULTIDISCIPLINARY JOURNAL VOL 2, ISSUE 3

GROWING RESPONSIBILITIES OF SECURITY INDUSTRY TOWARDS CYBER CRIME PREVENTION IN INDIA

VINAYAK REVJI GANDAL
Department of Commerce &
Research Centre,
Savitribai Phule Pune University.
K.M.C. College Khopoli,
Tal: Khalapur Dist: Raigad.
MS (**INDIA)**

DR. KALE PRALHAD BABAN
Research Guide,
Department of Commerce &
Research Centre,
Savitribai Phule Pune University.
MS (**INDIA)**

ABSTRACT

Security Industry has always been an evolving profession, but technological advancement in the past 10 years have accelerated that change and dramatically altered the landscape of crime. Security industries are now expected to protect and prevent their community members from local offender's committing traditional crimes, as well as computer hackers. This new cyber threat has developed so quickly that local security agencies haven't had time to fully prepare themselves and identify their role in preventing and investigating cyber crimes that are committed. The IT infrastructure provides transmission and storage of gigantic amounts of critical information used in each domain of society and it enables government and private agencies to speedily interact with each other as well as with industry, citizens, state, local governments and across international boundaries. As technology increases the more people are connected and shared their information through internet. The chances of misusing their information also increases hence here comes a new name to a crime that is cybercrime. Cybercrime being global and a very big threat now a days for all over the world, generally affects the person far away from the place of offence. The paper focuses on various types of cyber crime, role of security industry, challenges faced by people, security industry and government related to cybercrime in India.

Key Words: *Security Industry, Cyber crime, Challenges, Cyber security, law enforcement agencies etc.*

INTRODUCTION:

Due to lack of information security various cyber crimes arises. According to Sunit Belapure and Nina Godbole Cyber security means the set of activities, technical and non-technical

aspects of protecting information, devices, computer resources, network resources and other critical information stored there in from unauthorized access, modification and disruption, disclosure (qtd. In Ijarcsse 629). Crime is a major social and legal problem in the world we live in and population is one of the important factors, influencing incidence of crime. In current scenario cyber crime is increasing very fast as the technology is growing very rapidly. So the cyber crime investigation is becoming a very complicated task to do without a proper framework. There is wide range of different types of cyber crime today. Solution of each case requires a very complicated task. In preventing cyber crime, security industry has assumed a more critical role in recent years. With the increasing growth of Indian economy over last two decades, the requirement of security arrangement of Industrial Complex, Offices, Banks, IT Parks, ATM and other public infrastructure has grown manifold. In order to meet these demands, the security industry has significantly scaled its operational capabilities to supplement government towards maintaining safety and security of citizens and their properties. Norton's Cyber Crime Report 2011 reveals that India loses approximately INR 34,110 Crores annually due to cyber related crimes. Maintenance of security and law and order in the community is being undertaken by police organisations, but in the recent times we are witnessing an increasing trend towards the use of privately funded bodies, commonly referred to as 'private security' (Nalla, M. and Newman 13). Parfomak, Paul.W stated that, the evolution of private security helps the industries in the proportionate share of major security firms and providing private security services (qtd. In Paripex 170)

The paper is organized in five sections including the introduction. The second and third section includes types of cyber crime and role of security industry towards cyber crime prevention. In fourth section we have discussed the challenges. The fifth section concludes with summery of findings and suggestions for practice direction.

OBJECTIVES OF THE STUDY:

The following are the main objectives of the study:

1) To study the types of cyber crimes in India.
2) To study the role and responsibilities of security industry in cyber crime prevention.
3) To study the challenges of cyber crime.

RESEARCH METHODOLOGY:

The present research paper is based on secondary source of data. The secondary information has been collected from published books, articles published in different journals, various reports and websites.

TYPES OF CYBER CRIME:

There are many types of cyber crime prevailing in the system. Generally we can classify them in to following categories as discussed below:

CRIME AGAINST PERSON:

This type of crime includes various crimes such as harassing anyone with the use of computer that could be via e-mail. Cyber stalking and transmission of child pornography, Credit Card Fraud and Dissemination of obscene material including Software Piracy.

CRIME AGAINST PROPERTY:

It is the crime against all forms of property. These include computer vandalism, Intellectual Property Crimes, Threatening and Salami Attacks. This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes.

CRIME AGAINST ORGANIZATION:

Cyber Terrorism is one discrete kind of crime in this kind. The growth of internet has shown that the standard of cyberspace is being used by individuals and groups to pressure the international governments as also to terrorize the citizens of a country. In this crime a human being cracks in to a government, private organisation and military websites.

CRIME AGAINST SOCIETY:

In this type forgery, cyber terrorism, web jacking, polluting the Youth through Indecent, Financial Crimes, Sale of Illegal Articles, Net Extortion, Cyber Contraband, Data Diddling, Salami Attacks, Logic Bombs types of crime is included. Forgery currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers. Web Jacking hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

ROLE AND RESPONSIBILITIES OF SECURITY INDUSTRY:

The security industry in India adopted the methodology of detect, observe and report. The security personnel don't need to make arrest, but have the authority to make a citizen's arrest, by requesting a police officer. The main duty of security guards is to enforce company rules and can act to protect lives and property for which they have given some sort of training. The main role and responsibilities of security industry are:

- Protect people and the property of his contracted clients

- Prevention of an incident/offense before has occurred
- Observe and report during or after an incident/offense
- To investigate crime
- To identify problems and situations that are likely lead to crimes
- Reduce the opportunities for the commission of crimes through preventive patrol and other security measures
- Aid and cooperate with other agencies in implementing appropriate measures for prevention of crimes
- Aid individuals who are in danger of physical harm
- Create and maintain a feeling of security in workplace

CHALLENGES FACED BY SECURITY INDUSTRY:

Criminal investigations of cyber crimes are complex, as the criminal activity itself is borderless by nature (John Herhalt p 13). Although Security industries, Governments are actively focused on fighting and preventing cyber criminals from damaging infrastructure, the very nature of cyberspace poses a number of challenges to the implementation of cyber regulation in any country. Within cyberspace it is often difficult to determine political borders and culprits. Furthermore, the cyber criminal community and their techniques are continuously evolving, making it more challenging for government and other security industry to keep up with ever-changing techniques. As per the findings of study conducted by ASSOCHAM-Mahindra SSG, every month nearly 12,456 cases of cyber crimes registered in India and around 2277 complaints of online banking/credit/debit card fraud have been reported in year 2014. Cyber crimes in India may likely to cross the 3, 00,000 by 2015 growing at compounded annual growth rate of about 107 per cent.

Year	**No. Of Cyber crimes**	**No. Of websites hacked**
2011	13,303	21,699
2012	22,060	27,605
2013	71,780	28,481
2014 (Till May)	62,189	48,174
Total	1,69,332	1,25,959

Source: ASSOCHAM-Mahindra SSG study (Jan 2015)

The following are the various challenges faced by government and security industries while preventing cyber crime in India:

TRACKING THE ORIGIN OF CRIME:

Investigation of cyber crimes are complex, as the criminal activity itself is borderless by nature. So tracing cyber criminals poses a challenge.

GROWTH OF THE UNDERGROUND CYBER CRIME ECONOMY:

A major threat that may hamper the fight against cyber crime is the growth of an underground economy, which for many cyber criminals can be a lucrative venture. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiative. In the cyber underworld, the hackers and organized crime rings operate by selling confidential stolen intelligence.

SHORTAGE OF SKILED CYBER CRIME FIGHTERS:

Implementing cyber security measures requires skilled manpower. However, most countries face a shortage of skilled people to counter such cyber attacks.

WIDESPREAD USE OF PIRATED SOFTWARE:

One of the major challenges to preventing cyber crime is the prevalence of software piracy, as pirated software is more prone to attacks by viruses, malware and Trojans.

CONCLUSION:

Security industries and law enforcement agencies find it necessary to legalize the activities that influence our daily lives with the assistance of science. Laws are persistently being broadened and revised to defy the escalating crime rates. The security industry has a diverse but equally vital role to play in cyber security assurance in the form of long term strategies. The paper focuses on cyber crime, its classification and various challenges related to cyber crime and the role of security industry to combat the issue. The cyber crime can be classified in to four major categories such as Cybercrime against person, cyber crime against property, cyber crime against organization, cyber crime against society. In order to meet the challenges of cyber crime in India, it is essential to have a security industry which is up-to-date with modern techniques in its daily work.

REFERENCES

1) Anup Kumar Verma and Aman Kumar Sharma (2014): Cyber Security Issues and Recommendations, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 4, April, 2014. P 629.

2) Bhupinder singh Bhullar (2015): Growing Responsibilities of Private Security in India: Challenges and Suggestions, *Indian Journal of Research (Paripex)*, Volume 4, Issue 5, May, 2015. p 170.

3) John Herhalt (2011): Cyber Crime – A Growing Challenge for Government, KPMG International Cooperation, Canada, p 13.

4) Nalla, M. and Newman, G. (1990): A primer in private security, Harrow and Weston, New York, p 16.

5) Symantec Corporation, "Norton Cyber Crime Report 2011"; *www.symantec.com*

6) "Cyber crimes in India is likely to cross 3,00,000 by 2015: study (2015)" available at *http://www.assocham.org*